Biometric for Home Environment Challenges, Modalities and Applications

Ahmad Rabie
Institute of Computer Sciences
University of Applied Sciences Ruhr-West
Bottrop, Germany
ahmad.rabie@hs-ruhrwest.de

Uwe Handmann
Institute of Computer Sciences
University of Applied Sciences Ruhr-West
Bottrop, Germany
uwe.handmann@hs-ruhrwest.de

***Abstract*—Utilizing biometric traits for privacy- and security-applications is receiving an increasing attention. Applications such as personal identification, access control, forensics applications, e-banking, e-government, e-health and recently personalized human-smart-home and human-robot interaction present some examples. In order to offer person-specific services for/of specific person a pre-identifying step should be done in the run-up. Using biometric in such application is encountered by diverse challenges. First, using one trait and excluding the others depends on the application aimed to. Some applications demand directly touch to biometric sensors, while others don't. Second challenge is the reliability of used biometric arrangement. Civilized application demands lower reliability comparing to the forensics ones. And third, for biometric system could only one trait be used (uni-modal systems) or multiple traits (Bi- or Multi-modal systems). The latter is applied, when systems with a relative high reliability are expected. The main aim of this paper is providing a comprehensive view about biometric and its application. The above mentioned challenges will be analyzed deeply. The suitability of each biometric sensor according to the aimed application will be deeply discussed. Detailed comparison between uni-modal and Multi-modal biometric system will present which system where to be utilized. Privacy and security issues of biometric systems will be discussed too. Three scenarios of biometric application in home-environment, human-robot-interaction and e-health will be presented.**

I. Introduction

Automated biometric identification is a process of identifying someone based on one or more biometric traits. Typically and independent of the used trait, biometric systems perform three basic tasks, namely acquisition of user data, feature extraction and decision making [1]. Fig. 1 depicts a basic typical structure of a biometric system. Several preprocessing and enhancements steps and could be achieved in order to get features with reliable quality for the next steps. Extracted features - shape and texture information of face image, positions and forms of veins within finger and hand palm image, or iris structure are then compared with already saved features of the considered people in order to get the final decision of being identified/verified or not. Basically, biometric systems function in on of two modes. The verification, achieved by a verifier Fig. 1, compares a captured claimed identity with suitable one of the system database and results either identified or not. The identification, achieved by an identifier Fig. 1, searches all saved identities saved in the system database and gives the most similar identity to the captured one back, if found.

The following sections will give an overview about such possible challenges and how to handle with them. Section III will present few application of biometric systems. A small conclusion and will close the paper.

978-1-4673-6636-6/15/$31.00 ©2015 IEEE

II. Challenges

Several challenges are encountered by biometric systems. Actually, the way of considering and handling with these challenges depends mainly and totally on the application aimed to. These challenges range from the selecting of suitable sensors according to their physical characteristics to the steps of enhancing the captured data of the user to extracting the suitable information (features) from these data and finally to the way of making decisions.

A. Sensor Suitability

The selecting of sensors for biometric systems depends totally on the aimed application. For home environment application the sensors should operate in such a way that does not influence the life rhythm of the user negatively. Another kind of sensors, cameras for surveillance application, which could be used to capture face or gait image data. Such cameras should have the ability of delivering image data with a reasonable quality, needed for further processing. Yet another issue concerning the selecting of suitable sensor is the direct contact between it and the system user. Some sensors demand a direct contact to the user, such as finger print and hand tree, while other do not such as hand face, hand palm and iris. Hygienic issues should be considered by the latter, when such systems are applied for service for public use. Especially for application in home environment the sensors should be able to acquire biometric data of the user accidentally, which demands that the sensors should not have any direct contact to the user.

B. Uni- and Multi-modality

Biometrics could be used in a stand-alone mode (unimodal) or in a fused mode (multi-modal). Uni-modal biometric systems is challenged by multiple issues, such as noisy captured data, non-universality, upper bound of identification accuracy

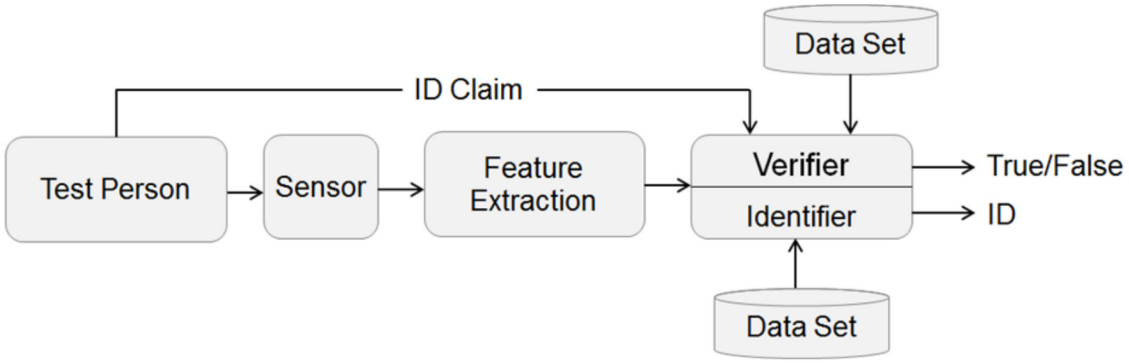

Fig. 1. Basic architecture of a biometric system. Person is either identified or verified.

and man-in-the-middle attacks. Some of these limitations of uni-modal systems can be avoided by realizing multi-modal system, which fuses input data of multiple biometric traits. Multi-modal biometrics fuses biometric traits at diverse levels in order to improve recognition accuracy. Fusion, i.e. Multi-modality, can either improve the performance of a uni-modal system, which could be degraded by noise or illumination, or reduce the number of false matches, which are caused by non-robust stand-alone biometric systems, or both. Multimodality can be accomplished by fusing two (bimodal) or more biometric traits (multi-modal) at several levels. In signal fusion level data from multiple sources are fused, as example raw data obtained using multiple sensors or multiple snapshots using single sensor. Multiple feature sets, which originate from multiple feature extracting algorithms, are gathered, normalized, transformed and dimensionally reduced to build a single feature set in the feature level fusion mode. Final decisions of multiple systems can be logically fused in the decision fusion level in order to get the final decision of the multi-modal system. Fig. 2 depicts the three possible levels of integrating multiple biometric subsystems in a single multimodal one.

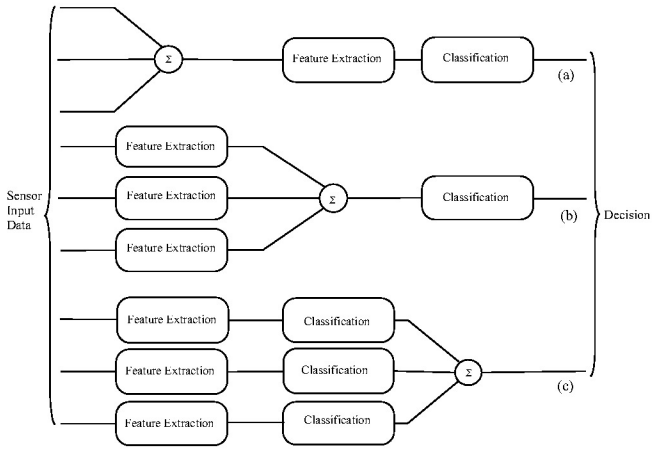

Fig. 2. Three basic fusion methods used in the current multimodal emotion recognition systems. $\sum$ presents signal, features and decision fusion levels in a, b and c respectively.

C. Trait Suitability

Most commonly used biometric traits are face, fingerprint, finger vein, hand palm, iris/retina, and voice. Employed biometric trait differs according to the aimed application and environment. For instance, adequate fingerprint samples require user cooperation; whereas, the face and iris images can be captured occasionally by a surveillance camera. Another issue, which influences the selecting of suitable trait is the operating range of system sensors. The majority of current iris cameras could perform well in a range up to 30 to 50 cm, while some surveillance cameras could have a range of two or even three digit number of meters. Therefor the former are suitable for security application application or the ones in home environment while the latter are more suitable for surveillance applications in airports and stadiums.

III. Application Scenarios

Wide range of biometrics applications are currently available on the market, under which surveillance systems, cash terminal with biometrics analysis abilities, biometrics-based payment systems[14], accessing digital systems, such as PCs, mobile phones and cars, accessing online services, such as online banking and personspecific services in home environment. In the following sections present some specific application of biometric system in home environment and e-health fields.

As we strive Towards our goal of presenting some biometric application for home environment and e-health application, we used the following scenarios the traits of face [2], finger vein [3], hand palm vein [4] to identify/verify the user. This selection fulfills the demand of the system being touch less, robust and multimodal.

A. Privacy-Aware Assisting System

In this work, we focused in this work on sustaining privacy issues of the user during a real interaction with the surrounding home environment [5]. A smart person-specific assistant system for services in home environment is proposed. The

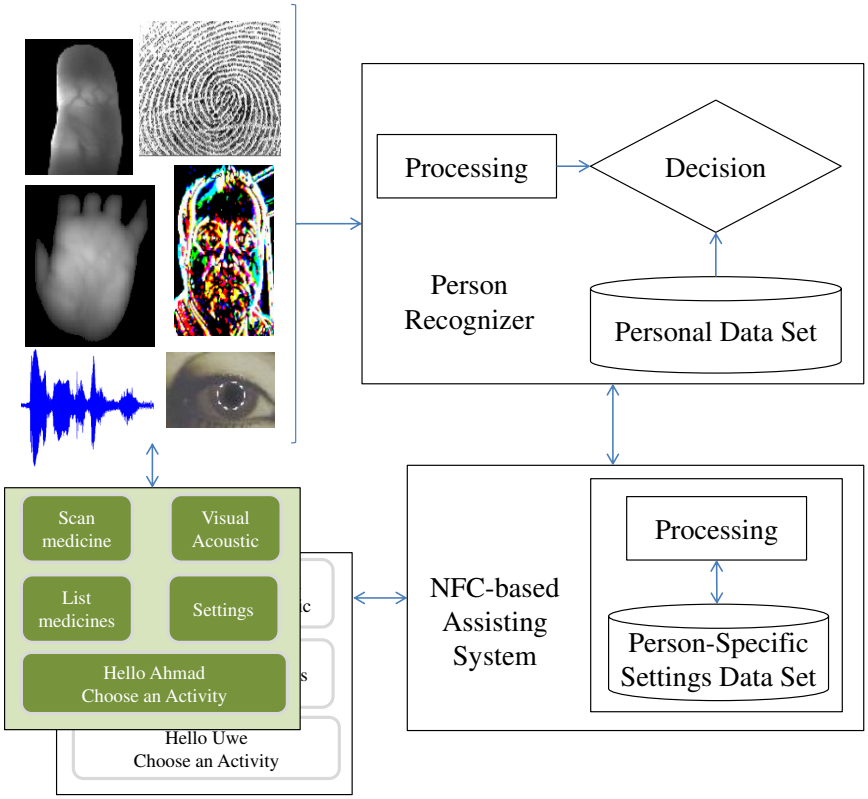

Fig. 3. Basic architecture of the medical assisting system. Person is identified by person recognizer, while the assisting system offers person-specific services.

role of this system is the assisting of persons by controlling home activities and guiding the adaption of Smart-Home-Human interface towards the needs of the considered person. At the same time the system sustains privacy issues of its interaction partner. As a special case of medical assisting the system is so implemented, that it provides for elderly or disabled people person-specific medical assistance. The system has the ability of identifying its interaction partner using some biometric features. According to the recognized ID the system, first, adopts towards the needs of recognized person. Second the system represents person-specific list of medicines either visually or auditive. And third the system gives an alarm in the case of taking medicament either later or earlier as normal taking time.

The basic structure of the whole system could be divided in two basic subsystems, person recognition subsystem and medicine organizer, as illustrated in Fig. 3. The former is based on the analysis of one or more biometric treats in order to identify the interaction partner, while the latter is a PC-tablet or smart phone equipped with modern utilities such as NFC and blue tooth. The system has the role of adapting according to the needs of its interaction partner. After the person is identified by the multi-modal biometric sub-system the assisting system modifies first the system-user interface accordingly. This modification could include the changing of system screening theme and interaction medium. Second the system serves the adapting of the surrounding environment towards the needs of its interaction partner. This could include the setting of heating and light conditions or even giving commands to prepare preferred meals or coffee. Socially the system could call the person-specific contact list and announce the daily arrangements, appointments and activities. Additionally the system sustains the privacy issues of multiple persons living in one household as it has the ability of connecting several portable devices according to the identified ID. Face, finger vein or hand palm vein data are acquired from the elderly interaction partner either deliberately or accidentally.

Once one or more of the above mentioned biometric features of the interaction partner are captured the suitable biometric features are extracted and analyzed by the corresponding person recognition subsystem and the final decision of the system is delivered as a person-ID to the service provider. The service provider (PC-tablet, smart phone), in turn, modifies first the theme of the interface in such a way, that it fulfills the needs of the recognized person. A list of persons-specific settings for the surrounding environment are then called and processed.

As a case study of a system we proposed a medical assisting system in a previous work [6]. The solely difference between both system is the function of them after the user is identified. According to the detected ID the system modifies the system theme adapting to user needs too. Additionally it presents a list of person-specific medicines either visually (on the screen) or acoustically (through speaker). Via an already established interface the medical assisting system will request the scanning of medicine packages. A smart device or PC-tablet with NFC ability is then used to scan the the NFC tag encapsulated into the package and extract ID of this medicine. Using a prior saved medicinal data set the medical organizer presents for the interaction partner the name of the medicine, how much times it is to be taken, last taking time and if it is presently due. The organizer has also the ability of giving an alarm if the considered medicine is wanted to be taken either too earlier or too later, as the taking time point saved in the medicinal data set.

B. e-Health system

In this scenario, biometric identification/verification serves both the goals of authenticating the reliability of collected data on the side of the patient and sustaining privacy and specificity issues of the patient on the side of health institute (hospital) [7]. On the side of patient, we employed the very well known biometric treat of face in addition to the traits of finger vein and palm vein. The reason for this is that these features dont demand any direct contact to the used sensor, which serve the goal of having a touch-less assisting system. All used traits are integrated in a single multi-modal biometric system by using a decision-level fusion method [6]. Considering the recently used health monitoring systems (smart mobile devices), which are equipped with diverse biometric sensors, such as camera for the capturing of face images or fingerprint sensor to acquire fingerprint data, the system proposed in [6] can be modified in two different ways. The first is to edit the biometric PC-Software in such a way, that it will be able to perform all steps of biometric identification locally. The second is just to acquire the biometric data through the sensors of the smart device and forward them to the central biometric server. The server will then process these data, extract some biometric features, get the ID of the person and send it back to the smart device. On the side of health institute camera and fingerprint sensor could be amounted to the central PC directly, which contains the central database of all patients of the institute and has the ability of identifying the responsible person using the same biometric system as on the side of patient. The privacy of the patient is still constantly sustained, as the access to private data of the patient depends on the identified personality of team member.

C. Human Robot Interaction

We focused in this work on the point that robot assisting systems with emotion understanding ability, which used currently in home environments, perform generally achieved in two several manners. The first is the implementing of such systems in such a way that they offer general services for all considered persons without considering privacy, special needs of their interaction partners. The second way is the targeting of such systems for merely one person. In this work we presented a robot assisting system, which has both the abilities of assisting several persons at the same time and sustaining their privacy and security issues [8]. The robot can interact with its interaction partner emotionally by analyzing the emotions of her expressed either visually, facial expression, or auditive, speech prosody [9]. The role of this system is the providing of person-specific support in home environment. In order to identify its interaction partner the system uses diverse biometric traits. According to the recognized ID the system, first, adopts towards the needs of recognized person. Second the system loads the corresponding emotional profile of the detected interaction partner in order to practice a person-specific emotional human-robot-interaction, which has an advantage over the person independent interaction.

IV. Conclusion

In this work we presented a small survey about biometrics. Encountered challenges, modalities and some applications for home environment are presented in this work. Biometric system, which fulfills the demand of being robust, reliable, operating accidentally and sustaining user privacy, are discussed. An application of biometric system in the field of e-Health is presented. The system serves both goals of confirming the reliability of patient data on the side of medical center and managing the access rights of the members of the medical center according to their rolls.

References

[1] A. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Springer, 2011.

[2] U. Handmann, S. Hommel, M. Brauckmann, and M. Dose, *Towards Service Robots for Everyday Environments*, ch. Face Detection and Person Identification on Mobile Platforms, pp. 227–234. Springer, 2012.

[3] N. Miura, A. Nagasaka, and T. Miyatake, "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification," *Machine Vision and Applications archive*, vol. 15, pp. 194–203, 2004.

[4] H. Zhang and D. Hu, "A palm vein recognition system," in *International Conference on Intelligent Computation Technology and Automation*, 2010.

[5] A. Rabie and U. Handmann, "Nfc-based person-specific assisting system in home environment," in *The 11th World Congress on Intelligent Control and Automation*, 2014.

[6] A. Rabie and U. Handmann, "Nfc-based person-specific medical assistant for elderly and disabled people," in *International Conference on Next Generation Computing and Communication Technologies*, 2014.

[7] A. Siddiqui, O. Koch, A. Rabie, and U. Handmann, "Personalized and adaptable mhealth architecture," in *5th International Conference on Wireless Mobile Communication and Healthcare*, 2014.

[8] A. Rabie and U. Handmann, "Multi-modal biometrics for real-life person-specific emotional human-robot-interaction," in *International Conference on Robotics and Biomimetics*, 2014.

[9] A. Rabie and U. Handmann, "Fusion of audio- and visual cues for real-life emotional human robot interaction," in *Annual Conference of the German Association for Pattern Recognition*, 2011.